Logistics and cloud computing service providers' cooperation: a resilience perspective

Article (Accepted Version)

Logistics and cloud computing service providers' cooperation: A resilience perspective

Nachiappan Subramanian*

Business Management and Economics,
University of Sussex
Falmer, Brighton BN1 9SL
N.Subramanian@sussex.ac.uk
Phone: +44 1273 872982

Muhammad D. Abdulrahman

Nottingham University Business School China,
The University of Nottingham Ningbo China,
199 Taikang East Road, Ningbo, 315 100.
muhammad.abdulrahman@nottingham.edu.cn
Phone: +86 574 8818 0019

* Corresponding Author

Submitted to the "Big Data and Analytics in Operations and Supply Chain Management" special issue of the Production Planning and Control journal

Logistics and cloud computing service providers' cooperation: A resilience perspective

Abstract

Cloud computing (CC) services can offer substantial cost-effective global operational and relationship benefits if the cooperation between logistics and CC services are resilient. Potential vulnerabilities to cooperation of CC and logistics service providers can occur with respect to vital factors such as security and trust. Extant studies have demonstrated CC benefits as well as few challenges associated with CC services application. However, no extant study has examined the inter-organisational benefits based on cooperative resilience between CC and logistics service providers in terms of both capability and trust vulnerability factors. This study examines the cooperative resilience of logistics and CC service providers based on innovation diffusion theory (IDT) within a supply-chain risk assessment framework. Using structural equation modelling techniques we investigate the relationship between the vulnerability factor (trust), capability factor (security) and collaboration benefits (relationship and operational) offered by CC service providers based on 236 Chinese logistics service firms' perceptions of cloud computing adoption. The results indicate Chinese logistics companies perceive security impediments as a major factor affecting cooperative resilience between logistics service and CC service providers.

Keywords: Logistics, cloud computing, cooperation, resilience, service provider

1. Introduction

The main objective of service providers' cooperation is to sustain the relationship by being able to predict and/or detect risks on time to deploy an appropriate response to prevent undesired impacts. However, not all risks and disruptions can be avoided, especially in the context of natural disasters. Two events that nearly totally disrupted cooperation of various service providers were the 2012 Hurricane Sandy and the 2011 Tsunami at Fukushima, Japan (DHS 2013). Sandy for example disrupted the electric grid outage to the communities in New York and New Jessy areas (Manual 2013) and transportation networks were disrupted due to huge storm-debris (Lipton 2013). These unavoidable and large-scale risks alerted each and every service provider of all regions to think about resilience strategies and be prepared to deal with response and recovery (DHS 2013; 2014). Resilience, the ability of an entity or system to return to normal conditions after the occurrence of an event that disrupts its state, is also at the heart of every contingency provision of a company, be it manufacturing or services, when deciding how it would prevent and/or respond to any form of disruptions to its supply chain systems (Hosseini, Barker, and Ramirez-Marquez 2016; Papadopoulos et al. 2016).

While earlier studies have been made regarding manufacturing firms, the manufacturing supply-chain network or humanitarian logistics; studies on the resilience of service providers' cooperation (Allenby and Fink 2000) are rare. In this study, we approach resilience from the perspective of the cooperation (i.e., continuous relationship and inter-dependency) between logistics and cloud service providers (CSPs). The transportation system is critical to the smooth flow of goods and services and the overall running of a modern infrastructure. However, the dependence of transportation systems on information and communication technology (ICT), especially cloud-based ICT, presents a unique risk and vulnerability than those traditionally associated with the transportation system itself; such as vehicle breakdown, extreme weather, bad roads or industrial strikes by the transport union. This is because, despite the acknowledged immense benefits ranging from flexibility to high scalability in the provisions of dynamic computing resources, how organisations deal with the challenges inherent in these innovation ecosystems remained unclear (Wamba et al. 2015). Specifically, CC is characterised by several concerns chiefly amongst which are security and trust capability of the service providers to protect critical business information (Morsy, Grundy, and Muller 2010; Bose, Luo, and Liu 2013).

We refer to CC in this study as an "IT service model where computing services are delivered on demand to customers over a network in a self-service mode, independent of device and location" (Marston et al 2011). When compared with traditional IT, CC has some special features such as ubiquity, resource-sharing, elasticity, low cost, and pay-per-use (Marston et al. 2011, Subramanian, Abdulrahman, and Zhou 2014). However, recurrent failures including service availability or reliability as well as outright data security and confidentiality breaches have been reported as unique risks associated with CC adoption (Subramanian, Abdulrahman, and Zhou 2014). In addition to security and trust issues, logistics firms face high vulnerability if cloud-based data communication which they heavily depend on is lost, especially in critical service operations (Clarke and Mosses, 2014).

Surprisingly, no past studies have investigated the continuing interdependence of logistics transport systems and CC service providers despite frequently reported real and perceived vulnerability and capability issues of CC service providers. This study aims to narrow this literature gap by examining the cooperation between CC service providers and their logistic transport service consumers in terms vulnerability and capability factors of security, trust and benefits (relationship and operational) associated with CC services. Understanding the continuing reliance of logistics service firms' on CC services despite reported inherent security, trust and reliability will provide key insights on the resilience of their cooperation. This study is important as literature suggests that resilience needs to build in terms of infrastructure security partnership (TISP 2006) as well as the capacity to avoid or protect against threats to revive critical services at a minimal impact or cost (Hosseini, barker, and Bamirez-Marquez 2016; Papadopoulos et al. 2016).

Furthermore, this study is particular relevant given the current reported state of local Chinese logistics firms' unorganised and operational inefficiencies that have resulted in poor customer satisfaction (KPMG 2011). Operational inefficiencies of Chinese logistics and transportation have been blamed on undeveloped infrastructure and resulting in high logistics costs of up to 18% of China's GDP (KPMG 2011). Despite the inefficacies of the sector however, The Global Intelligence Alliance (GIA) 2015 business perspectives on emerging markets suggest that transportation and logistics will contribute to 36% of global revenue in 2017, with China (along with Brazil, India and Russia) as the top contributors (GIA 2015) This is in line with Lin and Ho (2009) who suggested that the growth of China's economy depends largely on the extent and effectiveness of its logistics industry operation. The Asia Pacific FedEx Express (FedEx)

recently acknowledged that its operations within China are growing exponentially compared to other nations in the Asia-Pacific region (Cunningham 2012). This information led to our focus on China and specifically on this acknowledged critical sector of logistics transportation services to examining its perception on cooperative use of innovative technology such as CC services to achieve competitiveness and operational efficiency.

The rest of the study is structured as follows. Section 2 presents the review of the relevant CC literature and logistics service firms' cooperation. The third section presents the theoretical background of the study along with hypothesis development of the study. Section 4 presents details of the research methodology, followed by Section 5 presenting the results discussions. Finally, Section 6 provides the study's concluding remarks and its implications.

2. Literature review

Extant literature praised CC for its ability to deliver computing services directly and on demand to customers independent of device and location based on resource-sharing, elasticity, low cost, and pay-per-use (Marston et al. 2011). Literature further posits that the absence of pre-investment in infrastructure and related equipment which has significantly reduced financial burdens of enterprises needing to increase capabilities for the transferring of their services has motivated firms, especially small and medium enterprises (SMEs), to adopt CC (Marston et al. 2011). CC adoption also provides operational benefits through its ubiquity and device independence that has enabled strong business relationships between firms (Ren et al. 2015; Morgan and Hunt 1994). Despite the above benefits, however, extant studies suggest that CC also exposes its users to multiple challenges and/or concerns (Mansfield-Devine 2008). Some of the major concerns and challenges of CC adoption are security of data and trust, which are both critical for a firm in that there is high security and data is inaccessible to unauthorised users (Mansfield-Devine 2008).

2.1. Security and trust concerns

Information security and its assessment provide a fundamental basis for risk control and management (Mansfield-Devine 2008). Key security concerns for CC include issues such as

"privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support, and long-term viability" (Mansfield-Devine 2008). Extant study posits that the major factor against CC adoption is the security of business information (Morsy, Grundy, and Muller 2010; Bose, Luo, and Liu 2013). Security issues cut across all aspects of CC services: software security, platform security and infrastructure security; the details of which lay beyond the scope of this study (see: Morsy, Grundy, and Muller 2010; Bose, Luo, and Liu 2013; Julisch and Hall 2010; Kshetri 2013).

Trust (and commitment) is directly related to the establishment of successful cooperative behaviors (Morgan and Hunt 1994; Chen, Sohal, and Prajogo 2016). According to Morgan and Hunt (1994), trust will only be established when one party has confidence in an exchange partner's reliability and integrity. Literature identified trust (Siguaw, Simpson, and Baker 1998; Bose, Luo, and Liu 2013) as the second major CC services concern after security. These studies suggest confidentiality and privacy of data as important requirements that cloud service providers need to guarantee their customers to earn consumers' trust (Bose, Luo, and Liu 2013). There are several reasons why trust is a major issue for CC service. Firstly, CC is a new technology and to establish trust between a service provider and consumers who are autonomous entities and geographically separated is difficult. In fact, Bose, Luo, and Liu (2013) suggest that trust in CC can only be built gradually and over time through the service provider's reputation and actions. Other studies suggested the need for the CC service provider to establish a strong relationship by engaging in frequent communication with its customers to develop trust (Siguaw, Simpson, and Baker 1998; Bose, Luo, and Liu 2013).

However, several visible CC services failures such as spot failures or system outages seriously erode trust in CC service. Macías and Guitart (2016) posit that CC service providers can violate Service Level Agreement (SLA) with their clients through poor administrative control or even outright dishonest behaviour. A study by Alali and Yeh (2012) furthermore indicates that unclear or limited legal standards regarding compensation and responsibility coupled with a lack of regulatory guidance that support its users complicate trust issues.

2.2. Cooperation benefits

2.2.1 Operational benefits

It is quite obvious that the implementation of IT can be a significant source of competitive advantages to a firm operating in diverse market places (Yu 2015; Marston et al. 2011). This

explains logistics service providers' increased recognition of the need to adopt IT technologies to help with system wide approaches that involves transportation, warehousing and distribution in addition to effective communication with their business partners (Singh and Garg 2015; Hassan et al. 2015; Lin and Ho 2009). Even more interesting is the capability of CC solutions to offer these traditional IT services on demand at a much lower cost and on a pay-per-use basis. Literature suggests that CC solutions provide logistics service providers with unique capabilities to effectively organize and execute key activities such as handling, transportation, freight forwarding, customs clearance, warehousing, distribution, along with other value-added services and shared-work processes (Subramanian, Abdulrahman, and Zhou 2014). These are achieved through smart technologies such as radio frequency identification (RFID), global positioning system (GPS) and geographical information system (GIS), et.al, that enable an efficient logistics operation system with a high degree of customer satisfaction (Srivastava 2004). For example, RFID enables firms to interact with product items without physical contact, serving as a tool for real-time data communication in the supply chain (Attaran 2007). Additionally, GPS is an online tracking system that provides logistics enterprises with a real-time fleet management system (RTMFS) (Srivastava 2004).

CC based IT systems enable the logistics service providers to obtain these operational benefits of real-time monitoring and interaction of their day-to-day operations at a substantially minimal investment (Srivastava 2004). Obtaining operational efficiency without pre-investment in IT infrastructure as offered by CC is critical in today's dynamic markets, especially for the small and medium-sized (SMEs) logistics firms. In addition to other benefits, the lack of initial investment requirement has been a major motivation for SMEs to adopt IT and related equipment (Morsy, Grundy, and Muller 2010; Marston et al. 2011).

2.2.2 Relationship benefits

The success of any service business such as CC lies in the mutual benefits based upon the relationship between the service provider and its recipient. This explains past studies' claims that the sustainability of service business lays in the promotion of a good cooperative relationship between the service provider and receiver (Sugiyama, Shirahada, and Kosaka 2015).

Of critical importance in the service business relationship is the time dimension (Sugiyama, Shirahada, and Kosaka 2015). In the current global market, Information and Communication

Technologies (ICT) are widely used to achieve this time dimension efficiency. ICT provides "valuable, timely, and accurate information" to achieve competitiveness in terms of improved fleet management efficiency and customer satisfaction (Bayrak 2013; Srivastava 2004).

Close interaction between the business partners greatly enhance their collaborative relationship and cloud-based ICT (CC) has been specifically reported to enhance collaborative B2B relationships (Attaran 2007). It is not surprising therefore that international logistics giants such as FedEx, UPS and DHL have all heavily invested in and adopted such advanced systems to track and monitor their transport services and to develop a convenient and fast channel of communication with their customers(Srivastava 2004).

The analysis of the numerous studies listed above clearly demonstrates the benefits as well as the challenges associated with CC service application. Few of the studies investigated adoption factors alongside the barriers to adoption (Chong et al. 2009; Lin and Ho 2009; Bayrak 2013). A clear literature gap is that none of these studies examine the inter-organisational benefits with respect to cooperative resilience in terms of capability and trust vulnerability factors of the CC service provider. These studies missed opportunities to investigate the challenges associated with resilience of CC adoption, i.e. continuous cooperation benefits between the CC service provider and its customers. The current study aims to fill this gap by examining how CC service consumers, specifically logistics service providers, perceive the trade-off between trust vulnerabilities and capability factors for security on the part of CC service provider. The study specifically assesses the resilience of logistics and CC service providers cooperation based on IDT and supply chain risk assessment framework.

3. Theoretical background and hypotheses development

In the current global market, Information and Communication Technologies (ICT) are widely used in a number of industries, and provide "valuable, timely, and accurate information" to achieve competitiveness and wise decision-making (Bayrak 2013). Compared with traditional ICT solutions, CC offers superior advantages such as zero initial fixed cost requirements, scalability, operational efficiency and other benefits such as infrastructure maintenance.[12] Companies can achieve these competitive advantages through adopting CC services. Not surprisingly logistics service providers are migrating from traditional ICT to CC for more effective and efficient transportation, warehousing, retailing and communication (Lin and Ho 2009).

To assess resilience of a supply chain, Pettit, Fiksel, and Croxton (2010) proposed a generic framework with potential vulnerability and capability factors. We used Pettit, Fiksel, and Croxton (2010) framework to identify vulnerability and capability factors and the utilization of innovation diffusion theory (IDT) for technology adoption (Rogers 2013). IDT has been widely accepted as one of the most commonly applied theories in the study of technology adoption (Rogers 2013). Specifically, past studies have used IDT to examine CC adoption in logistics and supply chain context (Chong et al. 2009; Wu et al. 2013; Subramanian, Abdulrahman, and Zhou 2014). Wu et al 2013 used IDT to investigate CC support of supply chain management information system infrastructure. Chong et al 2009 employed IDT to investigate the relationship between supply chain factors and the adoption of e-collaboration tools. Furthermore, Subramanian, Abdulrahman, and Zhou (2014) used IDT to examine the integration of logistics and cloud computing service providers based on perceived benefits in the Chinese context. We specifically use IDT perspectives of 'advantages offered' and 'ease of use' to examine the use and resilience of CC services from the perspective of Chinese logistics service providers. According to Rogers (2013), if suggested innovation conflicts with firms' established systems or needs it is unlikely to be adopted. Rather than causing conflict though, CC services perfectly meet the needs and aspirations of the logistics firms. We therefore draw on IDT, based on the above-mentioned characteristics of advantages offered, its ease of use and compatibility with the aspirations of Chinese logistics firms. The conceptual model developed is shown in figure 1.

Insert Figure 1 about here

3.1 Hypotheses development

3.1.1 Security capability issues

The majority of CC service concerns are related to unauthorized access and the specific location from where the CC services are offered (Julisch and Hall 2010; Kshetri 2013). This is important because CC service providers may have multiple geographical locations for their servers and while stored data is controlled and/or governed by legislation of the country where these physically exist, there is no clear regulation on the same data with respect to the third-

country citizens who may own such data (Kshetri 2013). This amongst others has been the major concern of several major institutions like medical research centres and banks who handle highly sensitive data requiring top security and confidentiality (Julisch and Hall 2010).

For logistics firms, sudden data outages and lack of access when needed due to different sources such as the availability of the Internet, natural disasters like the 2012 Hurricane Sandy in the U.S. that adversely disrupted the supply network for months due to power outages, and possible antagonistic attacks and other threats (manual 2013; Lipton 2013), amongst others, represent major concerns. Additionally, the lack of security guarantees in the service level agreement (SLA) has seriously questioned CC service providers' capability to keep customers' data secured (Morsy, Grundy, and Muller 2010; Macías and Guitart 2016).

Collaborative security is capable of enhancing several operational benefits (Sultan 2011). CC infrastructure allows enterprises to achieve high efficiency through improving resource utilization (Aymerich, Fenu, and Surcis 2008) and boosting business intelligence application adoption (Xu et al 2009).

Based on these arguments, we propose:

H1: Perceived lack of security capability will negatively impact cooperation benefits and thereby indirectly reduce the resilience of cooperation between logistics service providers and CC service providers.

3.1.2 Trust vulnerability concerns

The operational success of any supply chain is dependent on the level of trust amongst its partners (Bendoly, Donohue, and Schultz 2006). Trust has also been recognised as a key to successful business relations and a major factor in shortening new product and/or service development period (Morgan and Hunt 1994; Hsieh 2013; Msanjila and Afsarmanesh 2011). However, inter-organisational trust is heavily dependent on a degree of reliability of the other party involved in the business or partnership and is based on rationality rather than emotions (Ashnai et al 2016; Beckett and Jones 2012). Thus, inter-organisational trust (at CC service user side, i.e. the logistics service provider) is the extent to which the logistics service provider hold positive expectations that it can rely rationally on the CC service provider to do exactly

what is expected to fulfil the logistics service provider's needs, given its proven capability (adapted from (Ashnai et al. 2016). For example, the transport system that relies on CC services expects the elimination or reduction of service disruption, degradations and other vulnerabilities resulting from CC service failures. However, such needed guarantee is not forthcoming due to a lack of security guarantees in the service level agreement (SLA) by CC service providers (Morsy, Grundy, and Muller 2010; Macías and Guitart 2016) coupled with inherent difficulties of establishing trust between parties that are autonomous entities and geographically separated (Bose, Luo, and Liu 2013).

Furthermore, CC services suffer from unclear or limited legal standards regarding compensation and responsibility to service consumers (Macías and Guitart 2016; Srivastava 2004). This is in addition to a lack of regulatory guidance to support CC users further substantially erodes trust in CC adoption (Alali and Yeh 2012). Furthermore, the lack of visibility and/or intangibility of CC services whereby all system checks such as testing and security measures verifications are completely outsourced to the CC service providers will not convince consumers to trust the system (Mansfield-Devine 2008).

Based on these arguments, we propose

H2: Perceived lack of trust vulnerability will negatively impact collaboration benefits and thereby indirectly reduce the resilience of cooperation between logistics and CC service providers.

Based on the trust vulnerability factors and security capability factor arguments, it can be inferred that highly secured systems are needed to strengthen the cooperation between logistics and CC service providers. Previous studies suggest that there should be a reasonable degree of reliability on CC services based on rational rather than emotional aspects (Ashnai et al 2016. Here rationality can be based on the security and reliability of the CC services. Thus, the extent to which the logistics service provider holds positive expectations and high trust on the CC service provider will depend on the service provider's proven security capability. We therefore hypothesis that:

H3: Perceived trust is positively related to perceived security, thereby indirectly indicating trust as the antecedent vulnerable factor for enhancing security capability.

4. Methodology

4.1. Instrument and data collection

This study utilized a large-scale survey method based on survey instruments adapted from published literature. The operational aspects of cooperation benefits were adapted from Lee, Chae, and Cho (2013), Zissis and Lekkas (2012), and Bayrak (2013). Relationship aspects of cooperation benefits items were adapted from Zissis and Lekkas (2012), Barnatt (2010), and Bayrak (2013). All items responses were measured on a five point Likert-scale (1 = strongly disagree to 5 = strongly agree). A summary of the scale of items used is shown in Table 1.

Insert Table 1 about here

Despite being adapted from literature, we pre-tested the survey instrument with seven local logistics firms to ensure clarity and understanding of potential respondents in terms of wording and the format used (Podsakoff et al. 2003). Minor translational issues raised in the pre-testing were cleared before the survey instrument was distributed. Interested respondents were promised a summary of the final study findings. As the instrument survey was conducted in Chinese, we employed back-translation method (Su and Parham 2002) to avoid linguistic or cultural differences in translation from English to Chinese using bilingual (English and Chinese language) experts.

Our respondents were identified randomly from the China logistics directory (http://www.6-china.com/company/) with significant infrastructure investment. Details of the respondents are shown in Table 2. Overall, a total of 1,002 firms engaged in logistics activities (transportation, warehousing, express delivery services, freight forwarding and customs clearance) drawn from this directory were contacted for the study. All firms in this study have established IT departments with an average of five IT personnel (see Table 2). A total of 273 completed surveys were returned of which 37 where unusable due to incomplete information. The 236 valid responses represent an overall response rate of 23.6%. Respondent profiles are shown in Table 2. The demographic characteristics of the respondents will be highly helpful to analyse group perspective and few characteristics could act as control variables and they are respondent

position, years of operation and IT department size.

Insert Table 2 about here

Following the recommendations of Podsakoff et al. (2003) we ensured simplicity and clarity of the instrument via pilot testing, maintained confidentiality of respondents and made sure only qualified respondents completed the survey. Respondents are anonymous and free to abstain from answering any part of the survey. The above steps help lower the potential for common-method bias. Using wave analysis (Rogelberg and Stanton 2007) of comparing data collected from early respondents with data from late respondents through a two-way t-test showed no significant differences eliminating the existence of bias. Furthermore, the result of the un-rotated factor loadings analysis showed no factor accounted for 50 percent or more of the variance; hence common-method bias is not an issue in this study (Podsakoff and Organ 1986).

5.2. Data Analysis and Results

Firstly, exploratory factor analysis (EFA) based on Principal Component Analysis with Varimax Rotation was carried out to identify the structure of the relationships between the scale items employed. In line with the conditions of EFA of parsimony and interpretation ability, a Varimax rotation that minimizes the number of variables with high loads in a factor was employed. Our EFA results indicate our scale items were loaded appropriately with their factors. Table 1 shows the means, standard deviations and Cronbach's alpha of our data variables that ranges from 0.701 to 0.847 indicating the study instrument has adequate reliability (Nunnally 1978).

Following EFA, based on confirmatory factor analysis (CFA) we established the convergent validity of the data using AMOS 20 (see Table 3). The result indicates all items loaded very well (0.52 or greater at $p < 0.01$) on their respective constructs. Furthermore, all factor coefficients obtained are greater than twice their respective standard errors (see Table 3 and figures 2f), further indicating convergent validity (Anderson and Gerbing 1988). Discriminant validity was assessed based on examining if the variance-extracted estimate is higher than the

squared correlations (Anderson and Gerbing 1988). To ensure no given item has higher loading with another construct other than its own, we checked their cross loadings based on the recommendations of (Henseler, Ringle, and Sinkovics 2009). Results show all items have their highest loadings on their designed constructs, providing additional support for discriminant validity. Table 4 shows the descriptive statistics and correlations among constructs.

Insert Table 3 about here

Insert Figures 2a, 2b & 2c about here

To examine our hypotheses, we employed a two-step process following Anderson and Gerbing (1988) recommendation. Firstly, we estimated the measurement model using AMOS 20. The estimated model result indicated a good fit with observed Relative chi square ($\chi 2/df$) = 2.01, Tucker-Lewis index (TLI) = 0.91, Comparative fit index (CFI) = 0.91 and, RMSEA = 0.065. All of these values are within acceptable limits in the literature (Dwyer, Schurr, and Oh 1987) suggesting that our model construct satisfies the reliability and validity criteria. Secondly, we estimated the structural model of the study; Figure 3 shows the study estimated path model. Summary results of the estimated model are shown in Table 5. The results for the structural model indicates a good fit with relative chi square ($\chi 2/df$) = 2.01, Tucker-Lewis index (TLI) = 0.91, Comparative fit index (CFI) = 0.91 and, RMSEA = 0.069. These values confirm to the model fit.

As can be seen from Table 5, a perceived lack of security capability of CC service provider impacts negatively on resilience of the service, where H1 ($\beta = 0.35$, $p = < 0.001$) is supported. Perceived lack of trust capability to cooperation, H2 ($\beta = 0.09$, $p = <0.001$), is not supported. However, perceived trust has a strong positive relationship with perceived security H3 ($\beta = 0.63$, $p = < 0.001$). The summary of our hypothesis testing is shown in Table 5.

Insert Tables 4 & 5 about here

Insert Figure 3 about here

5. Discussions

This study results support H1 which states that perceived lack of security capability of CC service provider negatively impacts the collaboration benefits of logistics and CC service providers there by indirectly reducing the resilience of collaboration. The implication is that firms may recognise potential benefits of CC as demonstrated in previous studies suggest that high inter-organizational cooperative relationship is enabled by internet based technologies such as CC (Aymerich, Fenu, and Surcis 2008; Rao, Perry, and Frazer 2003). The investigated firms also show clear advantages as demonstrated in the IDT perspectives of 'advantages offered' and 'ease of use' of CC services in line with literature that suggests the adoption of CC infrastructure allows enterprises to achieve high efficiency through improving resource utilization (Sultan 2011). The investigated firms want to boost their business intelligence and to easily expand their business operations and widen their range of business targets when required by deploying this highly scalable IT technology with no fixed capital investment. This is in addition to these SME operational benefits of low infrastructure investments as they cannot afford the high cost associated with traditional IT systems. However, their perceived lack of security capability from CC service providers is serving as a major impediment to embracing CC. This has indirectly hampered full cooperation with CC service providers thereby indirectly reducing the resilience of cooperation.

The above finding is in line with previous studies which suggest that users are uncomfortable with CC services especially as it relates to unauthorized access to critical data, and to location of the service (Wu et al. 2013; Julisch and Hall 2010). The Chinese logistics firms investigated were not so keen to adapt CC with a lack of clear regulation on ownership of their data coupled with a lack of visibility on how the data is handled by the service providers, as demonstrated by the latent variables in the security construct. Since most of the firms investigated are SMEs,

it is not surprising that most consider technological issues regarding data security and its potential disruption through lack of availability as a major concern to them also. Similar concerns were reported by other technology related studies Kshetri 2013; Wu et al. 2013).

Despite studies indicating trust as a major success factor in achieving successful and resilient supply chain integration (Chen, Wang, and Yen 2014; Beckett and Jones 2012), our result indicated a lack of support for H2 which posits that perceived lack of trust vulnerability will negatively impact the cooperation benefits and thereby indirectly reduce the resilience of cooperation between logistics and CC service providers. It is possible this result may be connected with the fact that respondents weigh security heavily before considering trust issues, as indicated in our H3 that posits perceived trust has a strong effect on perceived security. In other words, the result demonstrates that logistics services firms may have rationalized their lack of trust based on a perceived lack of security and reliability of the CC services provider, as indicated in a prior study (Ashnai et al. 2016). Effectively, given the inability to guarantee security and service availability, as well as the minimization of other vulnerabilities resulting from CC service failures in service level agreement (SLA) (Morsy, Grundy, and Muller 2010; Ashnai et al. 2016), users find no reason to contemplate any form of trust for the CC service. Effectively, CC services providers have failed to guarantee consumers any form of reliability in terms of consistent service delivery or that the risking consumers will be treated well under new conditions in a benevolence manner (Hsieh 2013). CC service providers therefore need to find ways to build more verifiable security measures and assurances that will instil confidence in their service users.

This above analysis has focused on long-term business relationships between logistics and CC service providers in relation to their inter-organisational trust-based security and reliability of CC services offered. However, for the short-term relationship, inter-organisational trust and reliability may be a less critical issue because of the lack of substantial engagement duration to develop and therefore warrant any rational and objective assessment of trust (Dwyer, Schurr, and Oh 1987, Ashnai et al 2016). In addition, short-term business relationships are characterised by less commitment and less investments (Dwyer, Schurr, and Oh 1987), making short term inter-organisational relationships easily dissolved for even any slight dissatisfaction (Ferguson and Johnson 2011).

6. Conclusions

Our study analyses the cooperation benefits using capability and vulnerability factors that indirectly reflect resilience. For Chinese small and medium-sized logistics companies, their continued reliance on CC depends on their perceived relationship with and the operational benefits of CC services coupled with the CC service provider's capabilities in terms of security and vulnerability towards trust for their business. Thus, in terms of resilience, perceived risks and perceived trust of the service provider are critically important for logistics companies. The findings of this research provide both the CC service providers and their Chinese logistic service providers counterparts with a greater understanding of how the two services can cooperatively enhance their business operations. CC service providers can now understand the perceived antecedents of their services that encompass their capability in terms of security and deal with vulnerable trust aspects based on the cooperation benefits that the Chinese logistics and transport services providers perceive from CC services. The combined capability and vulnerability impacts determine the adoption and resilience of the business cooperation. Specifically, CC service providers would benefit from enhanced cooperation with logistics service providers through demonstrated elimination or minimisation of service disruption and failures associated with CC service. Customers' trust can be significantly improved through a reasonable level of guarantees in service level agreement (SLA) provided and by offering a greater level of transparency in the way their data is handled. Additionally, perceived security and trust can further be strengthened with the acceptance of a reasonable level of responsibility and provision of legally binding compensation to the customers when failures occur on the side of the CC service provider.

In summary, perceived security and trust are vital concerns that influence the resilience of logistics cloud users to continue to use CC. Cooperation benefits enhances logistics service providers' competitiveness and it is also the major challenge towards resilience of the Chinese logistics firms investigated in this study. Achieving cooperation benefits will enable logistics service providers to develop stronger resilience. This study is not without limitations. The study focused only on the logistics services sector. Given the ubiquity and universality of CC applications, there is a need for the extension of the study to other industries to establish the accurateness or otherwise of our findings. Moreover, even within the logistics sector investigated, our data covers only a limited number of firms drawn from 10 cities but other Chinese regions may present different situations, perhaps limiting the scope of this study's

findings. In addition to a large sample size, the use of other methodologies may benefit this study's findings. Furthermore, the study has investigated long-term inter-organisational relationship perspectives. It would be interesting to examine short-term inter-organisational relationships between the two service providers to see if there are any contrary findings. We must say that these limitations, however, do not negate the essence and value of this study since it has clearly provided both service providers, CC and logistics service managers clear perspectives under which they can perform competitively.

7. Future research direction

In the light of our investigations and findings, and in addition to the listed limitations of this study, we suggest future research direction to better prepare supply chain managers for the task of ensuring resilience against disruptions (manmade or natural disruptions) to their supply chain systems. Future research into establishing a collaborative multi-level security and trust framework between CC service providers and their service consumers is required as a basic requirement for a quick and dynamic formation of result-oriented collaborative network partners. Potential supply chain security/risk identification and mitigation framework should not be left for CC service providers initiatives alone, as what constitute supply chain risk exactly, which information should be monitored, and how risk mitigation should be designed is heterogeneous, with each firms taking a different perspective (Notteboom and Lam 2014, Heckmann et al. 2014; Ho et al. 2015). Therefore, collaborative multi-level security and trust identification and potential disruption mitigation framework that provide better assurances for both business partners should be explored.

Acknowledgement
We thank the special issue editors and anonymous reviewers for their constructive comments and encouragement. The comments were certainly helpful to improve the readability and quality of our manuscript.

References

Alali F.A., C.L. Yeh. 2012. "Cloud computing: Overview and risk analysis." *Journal of information systems* 26 (2): 13-33.

Allenby, B., J. Fink. 2000. "Social and ecological resilience: toward inherently secure and resilient societies." *Science* 24(3):347-364.

Anderson, J.C., and D.W. Gerbing. 1988. "Structural equation modelling in practice: A review

and recommended two-step approach." *Psychological Bulletin* 103(3):411-423.
Ashnai, B., S.C. Henneberg, P. Naudé, and A. Francescucci. 2016. "Inter-personal and inter-organizational trust in business relationships: An attitude-behavior-outcome model." *Industrial Marketing Management* 52: (2016) 128-139.
Attaran, M. 2007. "RFID: an enabler of supply chain operations." *Supply Chain Management: An International Journal* 12(4): 249-257.
Attewell, P. 1992. "Technology diffusion and organizational learning: The case of business computing." *Organizational Science* 3(1):1-19.
Aymerich, F.M., G., Fenu, and S. Surcis. 2008. "An approach to a cloud computing network." *Proceedings of the First International Conference on the Applications of Digital Information and Web Technologies* 113-118.
Barnatt, C. 2010. *A Brief Guide to Cloud Computing*. Robinson, London.
Bayrak, T. 2013. "A decision framework for SME Information Technology (IT) managers: Factors for evaluating whether to outsource internal applications to Application Service Providers." *Technology in Society* 35:14–21.
Beckett, R. C., & Jones, M. 2012. "Collaborative network success and the variable nature of trust." *Production Planning & Control* 23(4): 240-251.
Bendoly, E., Donohue, K., & Schultz, K. L. 2006. "Behavior in operations management: Assessing recent findings and revisiting old assumptions." *Journal of operations management* 24(6): 737-752.
Bose, R., X., Luo, and Y. Liu. 2013. "The Roles of Security and Trust: Comparing Cloud Computing and Banking." *The 2nd International Conference on Integrated Information*, *Social and Behavioral Sciences* 73: 30-34.
Chen, J. V., Wang, C. L., and Yen, D. C. 2014. "A causal model for supply chain partner's commitment." *Production Planning & Control* 25(9):800-813.
Chen, J., Sohal, A.S. and Prajogo, D.I. 2016. "Supply risk mitigation: a multi-theoretical perspective." *Production Planning & Control* 27(10) 853-863.
Chong, A.Y.L., K.B. Ooi, B., Lin, and S.Y. Tang. 2009. "Influence of interorganizational relationships on SMEs' e-business adoption." *Internet Research* 19:313-331.
Clarke, R., Moses L.B. 2014. "The regulation of civilian drones' impacts on public Safety." *Computer law & security review*, 30, 263 -285.
Cunningham, D. L. 2012. "FedEx Delivers in China" [Online]: http://www.chinabusinessreview.com/fedex-delivers-in-china/April 2012. (Access on July 2013).
Department of Homeland Security, DHS. 2013. "National Infrastructure protection plan." Washington, DC: Office of the Secretary of Homeland Security. http://www.dhs.gov/national-infrastructure-protection-plan (accessed December 13, 2015).
Department of Homeland Security, DHS. 2014. "Quadrennial homeland security review (QHSR)." Washington, DC: Office of the Secretary of Homeland Security. http://www.dhs.gov/quadrennial-homeland-security-review (accessed December 13, 2015).
Dwyer, F.R., P.H. Schurr, and S. Oh. 1987. "Developing buyer-seller relationships." *Journal of Marketing* 51(2): 11-27.
Farrell, J., and G. Saloner. 1985. "Standardization, compatibility, and innovation." *The RAND Journal of Economics* 16: 70-83.
Ferguson, J.L., and W.J. Johnston. 2011. "Customer response to dissatisfaction: a synthesis of literature and conceptual framework." *Industrial Marketing Management* 118-127.
Global Intelligence Alliance, GIA. 2015. "Growth Projected for Transportation and Logistics in Emerging Markets." https://www.intellitrack.net/growth-projected-for-transportation-and-logistics-in-emerging-markets.asp (accessed 09 January 2016).
Heckmann, I., T.Comes, and S. Nickel 2014. "A critical review on supply chain risk –

Definition, measure and modeling." *OMEGA: The International Journal of Management Science.*
Henseler, J., C.M. Ringle, and R.R. Sinkovics. 2009. "The use of partial least squares path modeling in international marketing." *Advanced in International Market* 20:277-320.
Ho, W., T. Zheng, H. Yildiz and S. Talluri. 2015. "Supply chain risk management: a literature review." *International Journal of Production Research* 53(16):5031-5069.
Hosseini, S. K., J.E. Barker, and Ramirez-Marquez. 2016. "A review of definitions and measures of system resilience." *Reliability Engineering and System Safety* 145: 47- 61.
Hsieh, K. N. 2013." The influence of inter-firm relationships on the outcome of new service development: a study of Taiwanese convenience store industry." *Production Planning & Control* 24(2-3): 172-180.
Julisch, K., and M. Hall. 2010. "Security and control in the cloud." *Information Security Journal* 19(6): 299-309.
Katz, M.L., and C. Shapiro. 1986. "Technology adoption in the presence of network externalities." *Journal of Political Economy* 94(4): 822-841.
Kilubi, I., and H. Haasis. 2015. "Supply chain risk management enablers - A framework development through systematic review of the literature from 2000 to 2015." *International Journal of Business Science and Applied Management* 10(1).
KPMG, 2011. "On the move in China—the role of transport and logistics in a changing economy." [Online]:http://www.kpmg.com/cn/en/issuesandinsights/articlespublications/pages/transport-logistics-in-china-201112.aspx Publication data: November 2011. Access on July 2013.
Kshetri, N. 2013. " Privacy and security issues in cloud computing: The role of institutions and institutional evolution." *Telecom Policy* 37:372–386.
Lee, S.G., S.H. Chae, and MK. Cho. 2013. "Drivers and inhibitors of SaaS adoption in Korea." *International Journal of Information Management* 33: 429-440.
Lin, C.Y., and Y. H. Ho. 2009. "RFID technology adoption and supply chain performance: an empirical study in China's logistics industry." *Supply Chain Management: An International Journal* 14 (5): 369-378.
Lipton, E. 2013. "Cost of storm-debris removal in city is at least twice the US average." *The New York Times.*
Macías, M., J. Guitart. 2016. "Analysis of a trust model for SLA negotiation and enforcement in cloud markets." *Future Generation Computer Systems* 55: 460-472.
Mansfield-Devine, S. 2008. "Danger in the clouds." *Network security* December 2008.
Manual, J. 2013. "The long road to recovery: environmental health impacts of hurricane sandy." *Environ Health Perspectives* 121: 152-159.
Marston, S., Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi. 2010. "Cloud computing - The business perspective." *Decision support system* 51: 176-189.
Morgan, R. M., and Hunt, S. D. 1994. "The commitment-trust theory of relationship marketing." *The journal of marketing* 58(3):20-38.
Morgan, R.M., and S.D. Hunt. 1994. "The commitment–trust theory of relationship marketing." *Journal of Marketing* 58(3):20-39.
Morsy, M.A, J. Grundy, and I. Müller. 2010. "An Analysis of The Cloud Computing Security Problem" *In Proceedings of APSEC 2010 Cloud Workshop*, Sydney, Australia, 30th Nov 2010.
Msanjila, S. S., and Afsarmanesh, H. 2011. " On modelling evolution of trust in organisations towards mediating collaboration." *Production Planning & Control* 22(5-6), 518-537.
Notteboom, T., and S. L. L. Jasmine. 2014. " Dealing with uncertainty and volatility in shipping and ports,." *Maritime Policy & Management* 41:7, 611-614.
Nunnally, J.C. 1978. *Psychometric Theory.* McGraw Hill, New York.

Papadopoulos, T., A. Gunasekaran, R. Dubey, N. Altay, S. J. Childe, and S. Fosso-Wamba. 2016. " The role of Big Data in explaining disaster resilience in supply chains for sustainability." *Journal of Cleaner Production.*

Pettit T.J., J. Fiksel, and K. L. Croxton. 2010. "Ensuring Supply Chain Resilience: Development of a Conceptual Framework". *Journal of Business Logistics* 31:1.

Podsakoff, P.M., and D. Organ. 1986. "Self-reports in organizational research: problems and prospects." *Journal of Management* 12:531-543.

Podsakoff, P.M., S.B. MacKenzie, J.Y. Lee, and N.P. Podsakoff. 2003. "Common method biases in behavioral research: a critical review of the literature and recommended remedies." *Journal of Applied Psychology* 88:879-903.

Rao, S., C. Perry, and L. Frazer. 2003. "The Impact of Internet Use on Inter-Firm Relationships in Australian Service Industries." *Australasian Marketing Journal* 11 (2):10-22.

Rogelberg, S.G., and J.M. Stanton. 2007. "Introduction: understanding and dealing with organizational survey nonresponse." *Organizational Research Methods* 10 (2):195-209.

Rogers, E.M. 2013. *Diffusion of innovations (5thed).* New York: Free Press.

Siguaw, J.A., P.M. Simpson, and T.L. Baker. 1998. "Effect of Supplier Market Orientation and Channel Relationship: the Distributor Perceptive." *Journal of Marketing* 62 (3): 99-111.

Srivastava, B. 2004. "Radio frequency ID technology: the next revolution in SCM." *Business Horizons* 47(6):60-68.

Su, C.T., and L.D. Parham. 2002. "Case report - generating a valid questionnaire translation for cross-culture use." *American Journal of Occupation Therapy* 56: 581-585.

Subramanian, N., M.D. Abdulrahman, and X. Zhou 2014. "Integration of logistics and cloud computing service providers: Cost and green benefits in the Chinese context." *Transportation Research Part E: Logistics and Transportation Review* 70: 86-98.

Sugiyama, D., K., Shirahada, and M. Kosaka. 2015. "Elements to organize the third place that promotes sustainable relationships in service businesses." *Technology in Society* 43: 115-121

Sultan, N.A. 2011. "Reaching for the "cloud": How SMEs can manage." *International Journal of Information Management* 31:272-278.

The infrastructure Security Partnership, TISP. 2006. "Regional disaster resilience: a guide for developing on action plan." *Reston, VA: American Society of Civil Engineers; 2006. The infrastructure Security Partnership.*

Wu, Y., G. Casey, C. Benjamin, T. Hazen, and D.J. Hall. 2013. "Cloud computing in support of supply chain information system infrastructure: understanding when to go to the cloud." *Journal of Supply Chain Management* 49 (3): 25-41.

Xu, M., D. Gao, C. Deng, Z. Luo, and S. Sun. 2009. "Cloud Computing Boosts Business Intelligence of Telecommunication Industry," in Proceedings of *the First International Conference on Cloud Computing* 224-231.

Zissis D., and D. Lekkas. 2012. "Addressing cloud computing security issues." *Future Generation Computer Systems* 28:583-592.

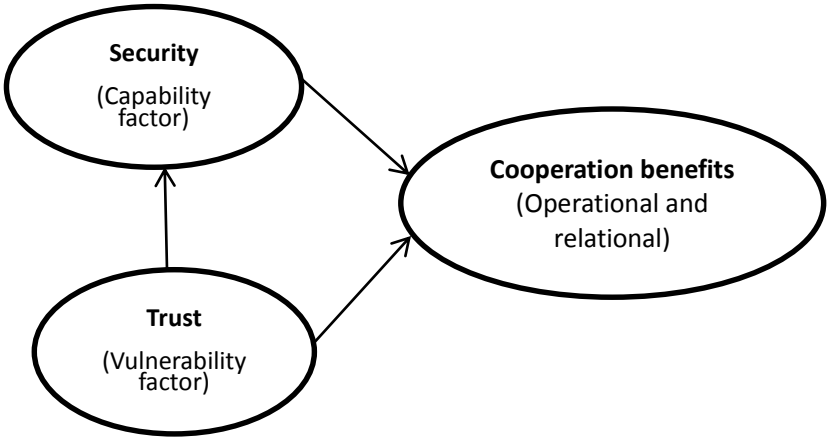

Figure 1: Conceptual model

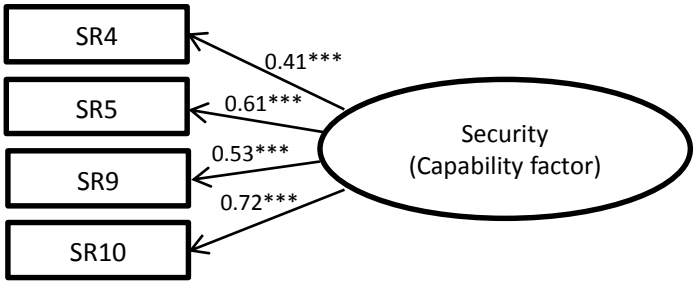

Figure 2 a: CC Security measurement model

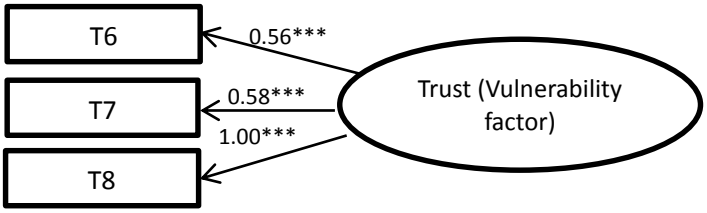

Figure 2b: CC Trust capability measurement model

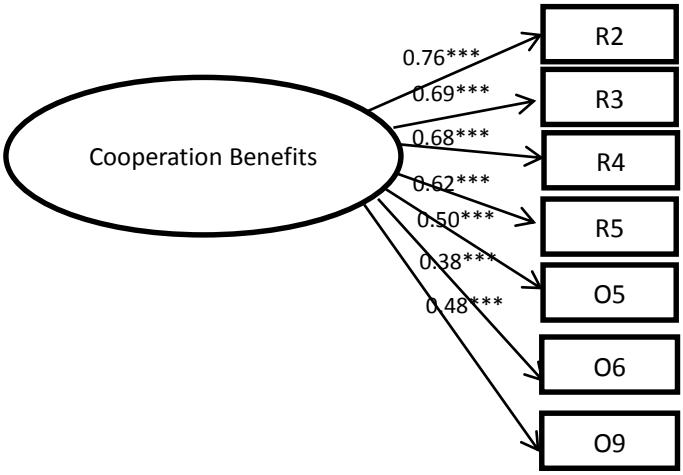

Figure 2c: CC Relationship benefits measurement model

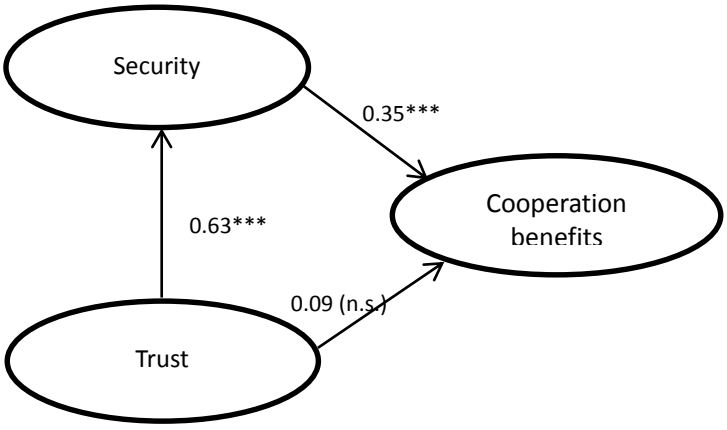

Figure 3: Path Model

Table 1: Scale Items

Items		Mean	SD	Cronbach's Alpha
Perceived Security				
SR4	Reliance on CC provider is a problem	3.71	0.90	0.803
SR5	Lack of visibility on data handling	3.72	0.84	
SR9	Too many technological issues regarding data security	3.56	0.81	
SR10	Lack of clear policy on data ownership	3.64	0.79	
Perceived Trust				
T6	Lack of government support policy	3.56	0.99	0.736
T7	Lack of service agreement for trial and evaluation	3.56	0.86	
T8	Lack of legal standards regarding compensation responsibility	3.66	0.90	
Cooperative (relationship + Operational) benefits				
R2	Close interaction between business partners	3.79	0.89	0.829
R3	Access to vital data anytime/anywhere will strengthened relationship	3.90	0.86	
R4	Access vital information will enhance stability of partnership	3.77	0.88	
R5	CC will provide ability to sustain Relationship	3.46	0.98	
O5	CC will enable us focus more on our core business	3.67	0.80	
O6	CC will increase process visibility across organizational boundaries	3.73	0.90	
O9	CC will enable us add or remove IT resource flexibly	3.58	0.84	

Table 2: Respondents' Profile

Characteristics	Total	Percentage (%)
Industry		
Express delivery services	77	32.6
Transportation, Warehousing, consolidation and distribution	159	67.4
Firm's Size (Number of employees)		
100 or fewer	81	34.3
101 and above	155	65.7
IT department size		
5 or fewer	107	45.3
6 and above	129	54.7
Years of operation		
< 10 years	108	45.8
11 and above	128	54.2
Respondent position		
IT Manager/ IT Support/Developer	118	50.1
Operations Manager	118	50.0
Total	236	100.0

Table 3 Confirmatory Factor Analysis Results

	Item	Std. Factor Loading
Perceived security	SR4: Reliance on CC Problem	0.41
	SR5: Lack of visibility in data handled	0.61
	SR9: Too many technological Issues on security	0.53
	SR10: Lack of clear policy on ownership	0.72
Perceived trust	T6: Lack of government support policy	0.56
	T7: Lack of service agreement	0.58
	T8: Lack of legal standards	1.00
Relationship benefits	R2: Close interaction partners	0.76
	R3: Access vital data anytime	0.69
	R4: Access vital Information enhance stability	0.68
	R5: Ability sustain relationship	0.62
Operational benefits	O5: Focus more on core business	0.50
	O6: Increase process visibility	0.38
	O9: Add or remove IT resources	0.48

All loadings are significant as $p<0.01$

Table 4 Correlation among construct

	SR4	SR5	SR9	SR10	T6	T7	T8	R2	R3	R4	R5	O5	O6	O9
SR4	1.00													
SR5	.237	1.00												
SR9	.270	.341	1.00											
SR10	.341	.417	.340	1.00										
T6	.198	.305	.384	.329	1.00									
T7	.158	.452	.422	.366	.523	1.00								
T8	.182	.390	.330	.470	.554	.575	1.00							
R2	.002	.166	.149	.147	.234	.232	.222	1.00						
R3	.121	.214	.187	.260	.259	.255	.229	.540	1.00					
R4	.093	.189	.240	.261	.242	.190	.221	.512	.468	1.00				
R5	.032	.175	.089	.080	.134	.143	.146	.513	.434	.372	1.00			
O5	.039	.066	.013	.122	.243	.095	.143	.380	.298	.410	.293	1.00		
O6	.056	.132	.141	.133	.261	.174	.148	.264	.235	.287	.235	.219	1.00	
O9	.115	.215	.249	.285	.225	.223	.231	.320	.312	.306	.361	.236	.159	1.00

Table 5 Hypotheses testing results

	Hypotheses	Unstd. Coefficient	Supported
H1	Security → Cooperation benefits	0.35***	Yes
H2	Trust → Cooperation benefits	0.09 n.s.	No
H3	Trust → Security	0.63***	Yes
N= 236; **p< 0.01;***p<0.001.			